

ABSTRACT OF THE DISCLOSURE

A method and system for distributed network address translation with security for controlling and limiting the disruption caused by denial of service attacks. The method and system have a first network device and a second network device on a first network, and a third network device on a second network external to the first network, with an established security association between the first network device and the third network device. The first network device specifies an external address of the third network device for the security association to the second network device, which stores the external address in a table. The second network device then maps at least one of an internal address and a security value to the external address in the table. Any packets sent from the third network device to the first network device are intercepted by the second network device, which determines the external address and security value of the packet. If the security value of the packet has been allocated to the first network device, and the external address of the packet has been specified by the first network device as being valid, the packet is sent from the second network device to the first network device using distributed network address translation with security. Otherwise, the packet is discarded by the second network device.